Notice of Allowability	Application No.	Applicant(s)	
	09/655,229	CHANG, CHUNG NAN	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Afterfinal Amendment filed on 10/23/06*.

2. ☒ The allowed claim(s) is/are *1-28*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

1. Claims 1-28 have been examined.

Allowable Subject Matter

2. The following is a statement of reasons for the indication of allowable subject matter: Claims 1-28 are allowable. The prior art of record discloses a protocol for cryptographic communication via a communication channel in which a sending cryptographic transmits onto the communication channel an encrypted ciphertext message obtained by supplying both a plaintext message and a cryptographic key to a first cryptographic device, and in which a receiving cryptographic unit receives the ciphertext message from the communication channel and by supplying the ciphertext message together with the key to a second cryptographic device decrypts the plaintext message therefrom, a method by which the sending unit and the receiving unit mutually establish a cryptographic key by first exchanging messages before the sending unit transmits the ciphertext message. In these protocols, a plurality of public quantities are made publicly available; the sending unit uses at least some of the plurality of public quantities in computing and transmitting to the receiving unit at least one sender's quantity; the receiving unit uses at least some of the plurality of public quantities in computing and transmitting to the sending unit at least one receiver's quantity; the receiving unit uses at least some of the plurality of public quantities and the plurality of sender's quantities in computing a session key. However, the prior art of record does not explicitly disclose the receiving unit transmitting for storage in a publicly accessible repository a plurality of public quantities computed from the at least some of the plurality of public quantities; the sender using at least one of the plurality of public quantities

to compute the key K; and the receiver uses at least one of the plurality of sender's quantities received from the sending unit to compute the key K. Therefore, claims 1-28 are allowable based on the reason stated above in light of other features disclosed in independent claims 1, 10, 19, and 28.

Response to Arguments

3. Applicant's arguments, see Remarks, filed 10/23/06, with respect to claim 28 have been fully considered and are persuasive. The rejection of claims 28 has been withdrawn. Furthermore, the rejection of claim 29 has been withdrawn because the claim has been cancelled.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100